Published and Copyright (c) 1999 - 2013
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1508 02/22/13

~ Rising Hacks Concern! ~ People Are Talking! ~ Yahoo Goes Social!
~ Commercial Cyberspying ~ April Xbox Unveiling? ~ PSN Gives Out Cash!
~ PlayStaion 4 Unveiled! ~ Anonymous A Hack Victim! ~ New Google 'Glass'!

-* Apple Hack Seems Familiar! *-
-* China Denies U.S. Hacking Charges! *-
-* U.S. Developing Penalties for Cybertheft! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""""

Here we go again!! For the past two weekends, we've been hit with some snow storms. First THE Blizzard of 2013 a couple of weeks ago, and then another heavy-ish storm last weekend.

All this week, I've been watching the local weather reports. Constant "updates" forecasting another big storm this weekend - with predictions of a foot or more of new snow. The forecasts have changed a little bit from day to day, but the totals stayed pretty much the same - until today. Today's forecast shows us that this pending storm has weakened significantly; and the new totals are down to about 3 - 6 inches. If so, it will just be more of an "annoyance" storm than anything else. But, having lived here in New England my entire life, I'll believe it when I see it!

I don't have much to discuss this week, but I do want to take this opportunity to do something that I don't always think to do. And that is to thank those folks who are avid A-ONE fans. Over the years, various readers have taken the time to communicate with us here, letting us know how they feel about our work, good or bad. And also, some have taken even more time to make contributions to us for inclusion in our issues, whether they be articles or notations of some interesting online articles for us to check out.

One such reader, Fred Horvat, has been providing A-ONE with articles for quite a few years now. While I don't know Fred personally (we've never met during Atari's heyday, or during the years since), have "talked" online via e-mails, etc. for quite some time. I just want to go on record, again, as thanking Fred for all of his help over the years. There have been many weeks in which A-ONE would have had very little content had it not been for Fred's contributions. In fact, there may have been some weeks in which an issue would not have appeared for lack of material. So, Fred, let me just offer a hearty thanks!

Until next time...

=~=~=~=

->In This Week's Gaming Section - PlayStation 4 Unveiled at NY Event!
""""""""""""""""""""""""""""""" Microsoft To Unveil Next Xbox in April!

PlayStation Is Giving Out Free Money!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
"""""""""""""""""""""""""""""""""""""

PlayStation 4 Unveiled at NY Event

Sony unveiled its next-generation gaming system, PlayStation 4, at an event in New York, saying the console will be part of a new ecosystem focused on hardware, software and "the fastest, most powerful gaming network."

"Our long-term vision is to reduce download times of digital titles to zero," said Mark Cerny, Sony's lead system architect on the PS4.

The new console is the Japanese electronics giant's first major game machine since the PlayStation 3 went on sale in 2006.

Wednesday's unveiling is Sony Corp.'s attempt to steal the spotlight, at least until Microsoft Corp. unveils its next Xbox in June, as expected, at the E3 video game expo in Los Angeles.

Among the PS4's revisions is an updated controller that adds a touchpad, motion control and a "share" button. The controller also features a light bar, which means a new PlayStation camera can more easily track the device.

Sony has struggled lately to keep up with Microsoft and other powerful rivals such as Apple Inc. and Samsung Electronics Co. The company is promising nifty mobile devices, sophisticated digital cameras and other gadgetry as part of its comeback effort.

The new device arrives amid declines in video game hardware, software and accessory sales. Research firm NPD Group said game sales fell 22 percent to $13.3 billion in 2012. One reason for the decline, analysts believe: It's been years since a new game machine was released. Most people who want an Xbox 360, PlayStation 3 or a Wii already have one. But people also have shifted their attention to games on Facebook, tablet computers and mobile phones. Sony and other game makers face the task of convincing people that they need a new video game system rather than, say, a new iPad.

Last fall, Nintendo started selling the Wii U, which comes with a tablet-like controller called the GamePad. It allows two people playing the same game to have entirely different experiences depending on whether they use the GamePad or a traditional Wii remote, which itself was revolutionary when it came out because of its motion-control features. The GamePad can also be used to play games without using a TV set, as one would on a regular tablet.

The original Wii has sold more units since its launch than both its rivals, but it has lost momentum in recent years as the novelty of its motion controller faded. Nintendo said it sold 3.1 million Wii Us by the end of 2012. It was a disappointing start for the first of a new generation of gaming systems.

In some ways, notably its ability to display high-definition games, the Wii U was just catching up to the PlayStation 3 and the Xbox 360, the preferred consoles to play popular games such as "Call of Duty" and "Red Dead Redemption."

All three console makers are trying to position their devices as entertainment hubs that can deliver movies, music and social networking as they try to stay relevant in the age of smartphones and tablets. The Wii U has a TV-watching feature called TVii. With it, the console's touch-screen GamePad controller becomes a remote control for your TV and set-top box. But Microsoft and Sony were ahead of the game in this front, too.

When the PlayStation 3 went on sale in the U.S. on Nov. 17, 2006, the 20 gigabyte model had a $500 price tag and the 60 GB version went for $600. They are now cheaper and come with more storage $270 for 250 GB and $300 for 500 GB. Comparable models of the Wii U and the Xbox 360 both start at $300.

Sony, meanwhile, started selling a mobile gaming device, PlayStation Vita, last February. The Vita connects to the PlayStation 3, so players can play the same game regardless of whether they are using a console or a handheld system.

Microsoft To Reportedly Unveil Next Xbox at April Event

The debut of Sony s PlayStation 4 is now behind us, so Microsoft is next in line to take a crack at grabbing gamers attention with its next-generation console. The Redmond, Washington-based company has worked its way to the top with its current-generation Xbox 360, which just recorded its twenty-fifth consecutive month as the best-selling console in the U.S. Now, according to a new report from Computer and Video Games, unnamed developers and other industry professionals including multiple Sony employees say Microsoft s next Xbox will be unveiled at a press conference in April. No other details were provided, but the next Xbox is expected to feature an eight-core 1.6GHz CPU, 8GB of RAM and a 50GB 6x Blu-ray Disc drive.

PlayStation Is Giving Out Free Money

In what you can only assume is a move to completely make February 20th all about PlayStation, Sony is giving certain PlayStation Network users free money. Just after midnight Central time in North America, certain PSN users found the following message in their inboxes along with a PSN code for $10.

Don't mind if I do...

No word on what the criteria is for getting the free money, but you'd assume it's for spending a certain amount of cash on the PlayStation Store as it's rewarding folks for being "a loyal customer." Sony has run programs in the past where spending a certain amount got you a certain amount of money back, but those programs are usually advertised.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

China Says U.S. Hacking Accusations Lack Technical Proof

Accusations by a U.S. computer security company that a secretive Chinese military unit is likely behind a series of hacking attacks are scientifically flawed and hence unreliable, China's Defense Ministry said on Wednesday.

The statement came after the White House said overnight that the Obama administration has repeatedly taken up its concerns about cyber-theft at the highest levels of the Chinese government, including with Chinese military officials.

The security company, Mandiant, identified the People's Liberation Army's Shanghai-based Unit 61398 as the most likely driving force behind the hacking. Mandiant said it believed the unit had carried out "sustained" attacks on a wide range of industries.

The Chinese Defence Ministry, which has already denied the charges, went further in a new statement, slamming Mandiant for relying on spurious data.

"The report, in only relying on linking IP address to reach a conclusion the hacking attacks originated from China, lacks technical proof," the ministry said in a statement on its website (www.mod.gov.cn).

"Everyone knows that the use of usurped IP addresses to carry out hacking attacks happens on an almost daily basis," it added.

"Second, there is still no internationally clear, unified definition of what consists of a 'hacking attack'. There is no legal evidence behind the report subjectively inducing that the everyday gathering of online (information) is online spying."

As hacking is a cross-border, anonymous and deceptive phenomenon, by its very nature it is hard to work out exactly where hacks originated, the statement said.

Chinese Foreign Ministry spokesman Hong Lei, asked about the U.S. taking up its concerns about hacking with Beijing, said: "China and the U.S. have maintained communication over the relevant issue".

Unit 61398 is located in Shanghai’s Pudong district, China’s financial and banking hub, and is staffed by perhaps thousands of people proficient in English as well as computer programming and network operations, Mandiant said in its report.

The unit had stolen "hundreds of terabytes of data from at least 141 organizations across a diverse set of industries beginning as early as 2006", it said.

Most of the victims were located in the United States, with smaller numbers in Canada and Britain. The information stolen ranged from details on mergers and acquisitions to the emails of senior employees, the company said.

But the Chinese Defence Ministry said China’s own figures show that a "considerable" number of hacking attacks it is subjected to come from the United States.

"But we don’t use this as a reason to criticize the United States," the ministry said.

However, the Global Times, a widely read tabloid published by Communist Party mouthpiece the People’s Daily, said China should be more active in publicly airing its complaints about hacking attacks, especially as the United States does so.

"Some officials have been punished for internally reporting that government websites have been hacked and secrets leaked, but almost no details have come out," it wrote.

"The Americans really know how to talk this (issue) up. All China can do is concede defeat."

Apple Hack Similar to Facebook Attack

Apple was targeted by the same hackers who went after Facebook last month, Reuters reported this afternoon and Apple confirmed to ABC News.

"Apple has identified malware which infected a limited number of Mac systems through a vulnerability in the Java plug-in for browsers," Apple said in a statement. "The malware was employed in an attack against Apple and other companies, and was spread through a website for software developers."

No data was stolen, Apple said. As in the Facebook case, the company said hackers were only able to access a small number of Apple employees’ Macintosh computers. Apple then isolated them from its network.

"There was no evidence that any data left Apple," the company said.

Facebook reported on Friday that it was "targeted in a sophisticated attack." Like Apple today, it said that there was no evidence that Facebook user data was compromised. Security experts told ABC News that it is likely that the only information compromised was what was on the personal computers of those employees whose machines were infected.

Both attacks used a vulnerability in Java, the software used to show much

of the content on Web browsers. Because of that vulnerability, the Department of Homeland Security released a statement last month urging computer users to disable the software in browsers.

Apple said that its operating systems do not ship with Java installed. If a user installs Java, Apple's software will automatically disable it if it has been unused for 35 days. Apple will also be releasing a new update that will help against Java threats.

"To protect Mac users who have installed Java, today we are releasing an updated Java malware removal tool that will check Mac systems and remove this malware if found," Apple said today.

Apple and Facebook's announcements comes after Twitter's announcement on Feb. 1 that 250,000 accounts were compromised in an attack. Twitter told affected users to reset their passwords. The New York Times and the Wall Street Journal said their computer systems were infiltrated by Chinese hackers in late January.

With so many security breaches, this is a good time to make sure you are following basic online safety tips - reset your passwords regularly, keep your anti-virus software up to date, and stay away from websites that seem questionable.

Rising Hack Attacks Prompt Concern

A string of hacking attacks at high-profile US companies has security experts and officials worried that the hackers are using information gained to plan even more sophisticated attacks.

Facebook announced it "was targeted in a sophisticated" attack last month, beginning a spate of high-profile hackings. The Twitter accounts of Burger King and Jeep were taken over by hackers earlier this week, just weeks after the site announced 250,000 user passwords had been compromised in an attack.

And on Tuesday, Apple confirmed the same hackers who went after Facebook had accessed a small number of Apple employees' Macintosh computers.

The Apple, Facebook and Twitter attacks could be related to an Eastern Europe operation, according to reports from Bloomberg and Reuters.

"That part of the world is without a doubt the most prolific and advanced center for criminal hacking on the planet," said Robert Siciliano, McAfee online security expert.

The social media hacks are separate from the alleged Chinese cyber espionage attacks detailed in a report released by Mandiant, a Virginia-based cyber security firm.

While there is a lot to sort out, here is what we know:

Apple and Facebook

No data was stolen in the Apple and Facebook hackings, according to both companies.

Security experts told ABC News that the only information likely compromised was on the personal computers of those employees whose machines were infected.

Both attacks used a vulnerability in Java, the software used to show much of the content on Web browsers. Because of that vulnerability, the Department of Homeland Security released a statement last month urging computer users to disable the software in browsers.

Apple said that its operating systems do not ship with Java installed. If a user installs Java, Apple's software will automatically disable it if it has been unused for 35 days. Apple will also be releasing a new update that will help against Java threats.

On Tuesday, Apple released an updated Java malware removal tool.

"The more data that these criminal hackers have, the more insight they have to the code of these different tech companies and how they do what they do and who the people on the inside are," Siciliano said. "All this intelligence is everything they need to build better hacking tools."

Twitter announced on Feb. 1 that 250,000 user passwords had been compromised, and said it had taken swift action, requiring a password reset before any hacked handle can be accessed again.

The breach was reportedly Twitter's largest data compromise to data, though the number of affected Twitter handles accounted for less than 0.125 percent of the service's 200 million active tweeters.

In a separate incident, the Burger King Twitter account @BurgerKing was hacked on Monday, with the logo, name and background page changed to McDonald's.

The hacker posted tweets that Burger King had been sold to McDonald's and the account had been taken over by McDonald's employees. "We just got sold to McDonalds! Look for McDonalds in a hood near you @DFNCTSC," the hacker tweeted at 12:01 p.m. ET. @DFNCTSC is likely an account set up by the hacker. Several of the posts used obscenities or racial epithets.

On Tuesday, Jeep became the second brand name to fall victim to a hacker, with a prankster taking over the account and suggesting the car company had been purchased by Cadillac.

Some unconfirmed reports suggested the Burger King hack had been perpetrated by the hacking group known as Anonymous.

Twitter is reportedly considering two factor authentication in order to help prevent hacks like Burger King and Jeep.

A report released by Mandiant, a Virginia-based cyber security firm, alleges a specific Chinese military unit is likely behind a cyber attack campaign that has stolen "hundreds of terabytes of data from at least 141 organizations" since 2006, including 115 targets in the U.S.

Mandiant's report was released a week after President Obama said in his State of the Union address that America must "face the rapidly growing threat from cyber attack."

"We know hackers steal people's identities and infiltrate private e-mail. We know foreign countries and companies swipe our corporate secrets. Now

our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy," he said.

President Obama pushed cyber security to the forefront last week, signing an executive order that will allow government agencies to work with private companies to tackle cyber threats.

Industries based in the U.S. will be asked to create voluntary standards for protecting information, while the federal government will commit to sharing cyber threat data with companies.

After the spate of hackings, Siciliano says personal users should be concerned and take precautions.

"When you have criminal hackers going after public-facing, consumer-oriented companies, the end game is to hack the public," he said.

Administration Developing Penalties for Cybertheft

Evidence of an unrelenting campaign of cyberstealing linked to the Chinese government is prompting the Obama administration to develop more aggressive responses to the theft of U.S. government data and corporate trade secrets.

The Obama administration is expected to announce new measures Wednesday, including possible fines and other trade actions against China or any other country guilty of cyber-espionage. Officials familiar with the administration’s plans spoke on condition of anonymity because they were not authorized to speak publicly about the threatened action.

The Chinese government denies being involved in the cyberattacks cited in a cybersecurity firm’s analysis of breaches that compromised more than 140 companies. On Wednesday, China’s Defense Ministry called the report deeply flawed.

Mandiant, a Virginia-based cybersecurity firm, released a torrent of details Monday that tied a secret Chinese military unit in Shanghai to years of cyberattacks against U.S. companies. Mandiant concluded that the breaches can be linked to the People’s Liberation Army’s Unit 61398.

Military experts believe the unit is part of the People’s Liberation Army’s cybercommand, which is under the direct authority of the General Staff Department, China’s version of the Joint Chiefs of Staff. As such, its activities would be likely to be authorized at the highest levels of China’s military.

The release of the Mandiant report, complete with details on three of the alleged hackers and photographs of one of the military unit’s buildings in Shanghai, makes public what U.S. authorities have said less publicly for years. But it also increases the pressure on the U.S. to take more forceful action against the Chinese for what experts say has been years of systematic espionage.

"If the Chinese government flew planes into our airspace, our planes would

escort them away. If it happened two, three or four times, the president would be on the phone and there would be threats of retaliation," said Shawn Henry, former FBI executive assistant director. "This is happening thousands of times a day. There needs to be some definition of where the red line is and what the repercussions would be."

Henry, the president of the security firm CrowdStrike, said that rather than tell companies to increase their cybersecurity, the government needs to focus more on how to deter the hackers and the nations that are backing them.

James Lewis, a cybersecurity expert at the Center for Strategic and International Studies, said that in the past year the White House has been taking a serious look at responding to China. "This will be the year they will put more pressure on, even while realizing it will be hard for the Chinese to change. There's not an on-off switch," Lewis said.

In denying involvement in the cyberattacks tracked by Mandiant, China's Foreign Ministry said China too has been a victim of hacking, some of it traced to the U.S. Foreign Ministry spokesman Hong Lei cited a report by an agency under the Ministry of Information Technology and Industry that said that in 2012 alone foreign hackers used viruses and other malicious software to seize control of 1,400 computers in China and 38,000 websites.

"Among the above attacks, those from the U.S. numbered the most," Hong said at a daily media briefing, lodging the most specific allegations the Chinese government has made about foreign hacking.

Cybersecurity experts say U.S. authorities do not conduct similar attacks or steal data from Chinese companies but acknowledge that intelligence agencies routinely spy on other countries.

China is clearly a target of interest, said Lewis, noting that the U.S. would be interested in Beijing's military policies, such as any plans for action against Taiwan or Japan.

In its report, Mandiant said it traced the hacking back to a neighborhood in the outskirts of Shanghai that includes a white 12-story office building run by the army's Unit 61398.

Mandiant said there are only two viable conclusions about the involvement of the Chinese military in the cyberattacks: Either Unit 61398 is responsible for the persistent attacks, or they are being done by a secret organization of Chinese speakers, with direct access to the Shanghai telecommunications infrastructure, who are engaged in a multi-year espionage campaign being run right outside the military unit's gates.

"In a state that rigorously monitors Internet use, it is highly unlikely that the Chinese government is unaware of an attack group that operates from the Pudong New Area of Shanghai," the Mandiant report said, concluding that the only way the group could function is with the "full knowledge and cooperation" of the Beijing government.

The unit "has systematically stolen hundreds of terabytes of data from at least 141 organizations," Mandiant wrote. A terabyte is 1,000 gigabytes. The most popular version of the new iPhone 5, for example, has 16 gigabytes of space, while the more expensive iPads have as much as 64 gigabytes of space. The U.S. Library of Congress' 2006-10 Twitter archive of about 170 billion tweets totals 133.2 terabytes.

Anonymous Becomes Latest Victim in Twitter Hacking Spree

Anyone who s ever had their website hacked and defaced by hacker collective Anonymous can have a good laugh at their expense, because it looks as though they aren t immune to security breaches either. BBC News reports that Anonymous this week has suffered an embarrassing breach, as one of its popular Twitter feeds is taken over by rival hacktivists. The Anonymous Twitter hack follows other high-profile Twitter hacks that have occurred over the past few days, including the Twitter accounts for both Burger King and Jeep. Graham Cluley, a senior consultant at security firm Sophos, tells BBC News that the hacks likely resulted from poor password practices, such as either using weak passwords or using the same password across multiple different accounts across the web.

Commercial Cyberspying, Theft Promise Rich Payoff

For state-backed cyberspies such as a Chinese military unit implicated by a U.S. security firm in a computer crime wave, hacking foreign companies can produce high-value secrets ranging from details on oil fields to advanced manufacturing technology.

This week’s report by Mandiant Inc. adds to mounting suspicion that Chinese military experts are helping state industry by stealing secrets from Western companies possibly worth hundreds of millions of dollars. The Chinese military has denied involvement in the attacks.

"This is really the new era of cybercrime," said Graham Cluley, a British security expert. "We’ve moved from kids in their bedroom and financially motivated crime to state-sponsored cybercrime, which is interested in stealing secrets and getting military or commercial advantage."

Instead of credit card numbers and other consumer data sought by crime gangs, security experts say cyberspies with resources that suggest they work for governments aim at better-guarded but more valuable information.

Companies in fields from petrochemicals to software can cut costs by receiving stolen secrets. An energy company bidding for access to an oil field abroad can save money if spies can tell it what foreign rivals might pay. Suppliers can press customers to pay more if they know details of their finances. For China, advanced technology and other information from the West could help speed the rise of giant state-owned companies seen as national champions.

"It’s like an ongoing war," said Ryusuke Masuoka, a cybersecurity expert at Tokyo’s Center for International Public Policy Studies, a private think tank. "It is going to spread and get deeper and deeper."

Mandiant, headquartered in Alexandria, Virginia, said it found attacks on 141 entities, mostly in the United States but also in Canada, Britain and elsewhere.

Attackers stole information about pricing, contract negotiations, manufacturing, product testing and corporate acquisitions, the company

said. It said multiple details indicated the attackers, dubbed APT1 in its report, were from a military unit in Shanghai, though there was a small chance others might be responsible.

Target companies were in four of the seven strategic industries identified in the Communist Party's latest five-year development plan, it said.

"We do believe that this stolen information can be used to obvious advantage" by China's government and state enterprises, Mandiant said.

China's military is a leader in cyberwarfare research, along with its counterparts in the United States and Russia. The People's Liberation Army supports hacker hobby clubs with as many as 100,000 members to develop a pool of possible recruits, according to security consultants.

Mandiant said it traced attacks to a neighborhood in Shanghai's Pudong district where the PLA's Unit 61398 is housed in a 12-story building. The unit has advertised online for recruits with computer skills. Mandiant estimated its personnel at anywhere from hundreds to several thousand.

On Wednesday, the PLA rejected Mandiant's findings and said computer addresses linked to the attacks could have been hijacked by attackers elsewhere. A military statement complained that "one-sided attacks in the media" destroy the atmosphere for cooperation in fighting online crime.

Many experts are not swayed by the denials.

"There are a lot of hackers that are sponsored by the Chinese government who conduct cyberattacks," said Lim Jong-in, dean of Korea University's Graduate School of Information Security.

The United States and other major governments are developing cyberspying technology for intelligence and security purposes, though how much that might be used for commercial spying is unclear.

"All countries who can do conduct cyber operations," said Alastair MacGibbon, the former director of the Australian Federal Police's High Tech Crime Center.

"I think the thing that has upset people mostly about the Chinese is ... that they're doing it on an industrialized scale and in some ways in a brazen and audacious manner," said MacGibbon, who now runs an Internet safety institute at the University of Canberra.

China's ruling party has ambitious plans to build up state-owned champions in industries including banking, telecoms, oil and steel. State companies benefit from monopolies and other official favors but lack skills and technology.

Last year, a group of Chinese state companies were charged in U.S. federal court in San Francisco in the theft of DuPont Co. technology for making titanium dioxide, a chemical used in paints and plastics.

In 2011, another security company, Symantec Inc., announced it detected attacks on 29 chemical companies and 19 other companies that it traced to China. It said the attackers wanted to steal secrets about chemical processing and advanced materials manufacturing.

In Australia, a report by the attorney general this week said 20 percent of 225 companies surveyed had experienced a cyberattack in the previous

year.

Australian mining companies make a tempting target because of their knowledge about global resources, said Tobias Feakin, head of national security at the Australian Strategic Policy Institute, a think tank.

As Chinese resource producers expand abroad, "you could see the motivation for understanding the Australian competition and infiltrating their systems," Feakin said.

China has long been cited by security experts as a center for Internet crime. They say some crimes might be carried out by attackers abroad who remotely control Chinese computers. But experts see growing evidence of Chinese involvement.

Few companies are willing to confirm they are victims of cyberspying, possibly fearing it might erode trust in their business.

"When companies admit their servers were hacked, they become the target of hackers. Because the admission shows the weakness, they cannot admit," said Kwon Seok-chul, president of Cuvepia Inc., a security firm in Seoul.

An exception was Google Inc., which announced in 2010 that it and at least 20 other companies were hit by attacks traced to China. Only two other companies disclosed they were targets. Google cited the hacking and efforts to snoop on Chinese dissidents' email as among reasons for closing its China-based search service that year.

Mandiant cited the example of an unidentified company with which it said a Chinese commodity supplier negotiated a double-digit price increase after attackers stole files and emails from the customer's chief executive over 2‰ years beginning in 2008.

"It would be surprising if APT1 could continue perpetrating such a broad mandate of cyberespionage and data theft if the results of the group's efforts were not finding their way into the hands of entities able to capitalize on them," the report said.

NYPD, Microsoft Create Crime-fighting Tech System

A 911 call comes in about a possible bomb in lower Manhattan and an alert pops up on computer screens at the New York Police Department, instantly showing officers an interactive map of the neighborhood, footage from nearby security cameras, whether there are high radiation levels and whether any other threats have been made against the city.

In a click, police know exactly what they're getting into.

Such a hypothetical scenario may seem like something out of a futuristic crime drama, but the technology is real, developed in a partnership between the nation's largest police department and Microsoft Corp., and the latest version has been quietly in use for about a year.

The project could pay off in more ways than one: The NYPD could make tens of millions of dollars under an unprecedented marketing deal that allows Microsoft to sell the system to other law enforcement agencies and civilian companies around the world. The city will get a 30 percent cut.

The Domain Awareness System, known as the dashboard, gives easy access to the police department’s voluminous arrest records, 911 calls, more than 3,000 security cameras citywide, license plate readers and portable radiation detectors. This is all public data not additional surveillance.

Right now, it is used only in NYPD offices, mostly in the counterterrorism unit. Eventually, the system could supply crime-fighting information in real time to officers on laptops in their squad cars and on mobile devices while they walk the beat.

"It works incredibly well," said Jessica Tisch, director of planning and policy for the counterterrorism unit.

For example, officers used the system during a deadly shooting outside the Empire State Building in August. Dozens of 911 calls were coming in, and it initially looked like an attack staged by several gunmen. But officers mapped the information and pulled up cameras within 500 feet of the reported shots to determine there was only one shooter.

Analysts are cautious about the potential profits, saying that largely depends on Microsoft’s sales efforts and whether any major competition arises. While there other data-drilling products made by other companies, they say the NYPD’s involvement could set the dashboard apart.

"This is the kind of stuff you used to only see in movies," said analyst Rob Enderle of Enderle Group, a technology analysis firm. "Getting it to work in a way that police departments can use in real time is huge."

The venture began in 2009 when the NYPD approached Microsoft about building software to help mine data for the Lower Manhattan Security Initiative, a network of private and public cameras and other tools monitored by the department’s counterterrorism bureau. Development cost the department between $30 million and $40 million, officials said.

"Usually, you purchase software that you try to work with, but we wanted this to be something that really worked well for us, so we set about creating it with them," said Richard Daddario, the NYPD’s deputy commissioner for counterterrorism.

Officers were involved throughout the process with the programmers, offering advice on what they need during an emergency.

"It was created by cops for cops," Tisch said. "We thought a lot about what information we want up close and personal, and what needs to be a click away. It’s all baked in there."

The system uses hundreds of thousands of pieces of information. Security camera footage can be rewound five minutes so that officers can see suspects who may have fled. Sensors pick up whether a bag has been left sitting for a while. When an emergency call comes in, officers can check prior 911 calls from that address to see what they might be up against.

Prospective clients can customize it to fit their organization.

Dave Mosher, a Microsoft vice president in charge of program management, said the company started to market the system in August and is looking at smaller municipalities, law enforcement agencies and companies that handle major sporting events.

He would not say whether any clients have been lined up and would not give details on the price except to say that it would depend on how much customization must be done.

Shawn McCarthy, an analyst with the research firm IDC, described the partnership and outcome as unusual in the tech world. "I see huge potential, but so much depends on the price and competition," he said.

No firm timetable has been set on when the dashboard will be rolled out to the entire 34,000-offficer department.

Yahoo Goes Social, Teams with Facebook for Site Revamp

Yahoo Inc is overhauling its website to incorporate features familiar to Facebook users such as a newsfeed and people's "likes," in CEO Marissa Mayer's biggest product revamp since taking the helm of the ailing company last year.

Mayer, who took over in July after a procession of CEOs was shown the door, said in a blog post on Wednesday that Yahoo's redesigned website will let users log in with their Facebook IDs to gain access to content and information shared by friends - from articles and videos to birthdays.

Yahoo is one of the world's most-visited online properties, but revenue has declined in recent years amid competition from Google Inc and Facebook Inc.

The changes to Yahoo's Internet shop window, which include a more streamlined mobile application for smartphones and tablets, will be rolled out over coming days. The makeover follows a new version of Yahoo mail, one of its most popular applications, introduced in December.

Analysts say the move marks a strengthening of Yahoo's ties with Facebook, employing some of the social network's growing data on its billion-plus users to battle Google for Web users' attention. It remains to be seen whether the initial makeover and tweaks expected over time will win back its Internet audience.

"This is definitely an important step. The Yahoo home page is one of the most important things because it is the first interface," said B. Riley Caris analyst Sameet Sinha. "It's familiar in terms of layout, the newsfeed is interesting, and it will be interesting to see how it develops over time.

"The key will be how data is aggregated within Yahoo and Facebook."

Seven months into her tenure, former Google executive Mayer has arrested the decline of the Internet portal and won favor on Wall Street with stock buybacks among other things. But Yahoo's forecast of a modest revenue uptick this year still pales in comparison with the growth of rivals like Google and Facebook, which are eating into its advertising market share.

"We wanted it to be familiar but also wanted it to embrace some of the modern paradigms of the Web," Mayer said of the product revamp on NBC's "Today" show on Wednesday.

"One thing that I really like is this very personalized newsfeed; it’s infinite and you can go on scrolling forever," she said.

Among other problems, Yahoo has been plagued by internal turmoil that has resulted in a revolving door of CEOs. Mayer, 37, took over after a tumultuous period during which former CEO Scott Thompson resigned after less than six months on the job over a controversy about his academic credentials. Yahoo co-founder Jerry Yang then resigned from the board and cut ties with the company.

Thompson’s predecessor, the controversial and outspoken Carol Bartz, was fired over the phone for failing to deliver on growth. Yahoo’s 2012 revenue was $5 billion. It has been flat year over year, off from some $6.3 billion in 2010.

Inside View on New Google Glass

Google has been showing off its glasses or its Project Glass for nearly a year now, but we haven’t seen much about what it looks like when you put on the futuristic, Internet-connected glasses that show digital information right in front of your eyes, projected over the physical world. Until today that is.

Google has launched a new website and a series of videos which show off features of the glasses - or what it is now officially calling Glass. As you can see in the video below, the glasses can be controlled with your voice and then a small box appears in the right hand corner of the glasses showing the software.

For instance, you can tell Glass to record a video or search for photos of tigers. Even more impressive seems to be the navigation functionality. You can tell Glass where you want to go and it will show a 3D navigation view in the corner. The video also shows what happens when you get a message - it pops up with the photo of the person, again in the right corner.

The glasses, Google told ABC News last year, have smartphone parts - a processor and battery - in the left leg. On the front of the glasses, in the top left (or right depending on which way you view them) corner is a small camera and a glass-looking box, which is a tiny display. On the top of the glasses is a power button and a camera button. You control the screen’s interface with the touchpad on the leg of the glasses.

With the new previews of the software and how it works, Google has also announced its plans to open up availability to real people. "We’re looking for bold, creative individuals who want to join us and be a part of shaping the future of Glass," Google writes on its Glass website. While Google has already started to test the glasses with software developers, they are now asking people to share on Google+ and Twitter their ideas of how they would use the glasses. Include the #ifihadglass hashtag and your idea in 50 words or less before Feb. 27 and Google might pick you. You can share them with Google on Google+ (+ProjectGlass) or Twitter (@projectglass).

Those selected will need to pre-order the developer version of the Glasses - called the Glass Explorer Edition - for $1,500. Google has already begun showing off the glasses to developers in New York and

San Francisco this month.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.